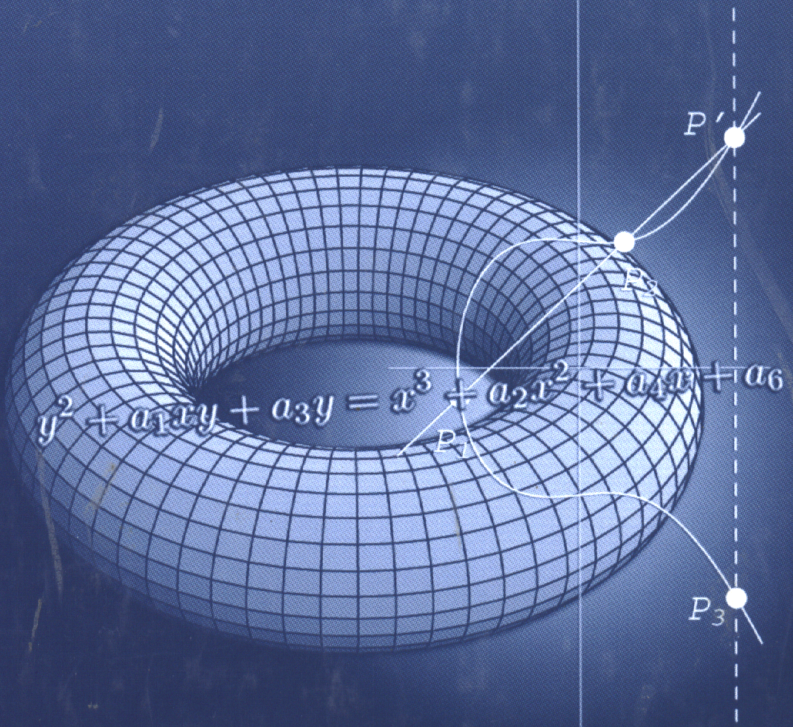
DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

ELLIPTIC CURVES

Number Theory and Cryptography



Lawrence C. Washington

CHAPMAN & HALL/CRC

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor

Kenneth H. Rosen, Ph.D.

AT&T Laboratories
Middletown, New Jersey

Applications of Abstract Algebra with Maple,
Richard E. Klima, Ernest Stitzinger, and Neil P. Sigmon

Algebraic Number Theory, *Richard A. Mollin*

An Atlas of Smaller Maps in Orientable and Nonorientable Surfaces,
David M. Jackson and Terry I. Visentin

An Introduction to Crytography, *Richard A. Mollin*

Combinatorial Algorithms: Generation Enumeration and Search,
Donald L. Kreher and Douglas R. Stinson

The CRC Handbook of Combinatorial Designs,
Charles J. Colbourn and Jeffrey H. Dinitz

Cryptography: Theory and Practice, Second Edition, *Douglas R. Stinson*

Design Theory, *Charles C. Lindner and Christopher A. Rodgers*

Enumerative Combinatorics,
Charalambos A. Charalambides

Frames and Resolvable Designs: Uses, Constructions, and Existence,
Steven Furino, Ying Miao, and Jianxing Yin

Fundamental Number Theory with Applications, *Richard A. Mollin*

Graph Theory and Its Applications, *Jonathan Gross and Jay Yellen*

Handbook of Applied Cryptography,
Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone

Handbook of Discrete and Combinatorial Mathematics, *Kenneth H. Rosen*

Handbook of Discrete and Computational Geometry,
Jacob E. Goodman and Joseph O'Rourke

Introduction to Information Theory and Data Compression, Second Edition,
Darrel R. Hankerson, Greg A. Harris, and Peter D. Johnson

Continued Titles

Network Reliability: Experiments with a Symbolic Algebra Environment,
Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt

RSA and Public-Key Cryptography
Richard A. Mollin

Quadratics, *Richard A. Mollin*

Verification of Computer Codes in Computational Science and Engineering,
Patrick Knupp and Kambiz Salari

Elliptic Curves: Number Theory and Cryptography
Lawrence C. Washington

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

ELLIPTIC CURVES

Number Theory and Cryptography

Lawrence C. Washington

CHAPMAN & HALL/CRC

A CRC Press Company
Boca Raton London New York Washington, D.C.

Library of Congress Cataloging-in-Publication Data

Washington, Lawrence C.
Elliptic curves : number theory and cryptography / Lawrence C. Washington.
p. cm. -- (Discrete mathematics and its applications)
Includes bibliographical references and index.
ISBN 1-58488-365-0 (alk. paper)
1. Curves, Elliptic. 2. Number theory. 3. Cryptography. I. Title. II. CRC Press Press series on discrete mathematics and its applications.

QA567.2.E44W37 2003
516.3'52--dc21 2003043972

International Standard Book Number 1-58488-365-0
Library of Congress Card Number 2003043972
Printed in the United States of America 2 3 4 5 6 7 8 9 0
Printed on acid-free paper

Preface

Over the last two or three decades, elliptic curves have been playing an increasingly important role both in number theory and in related fields such as cryptography. For example, in the 1980s, elliptic curves started being used in cryptography and elliptic curve techniques were developed for factorization and primality testing. In the 1980s and 1990s, elliptic curves played an important role in the proof of Fermat's Last Theorem. The goal of the present book is to develop the theory of elliptic curves assuming only modest backgrounds in elementary number theory and in groups and fields, approximately what would be covered in a strong undergraduate or beginning graduate abstract algebra course. In particular, we do not assume the reader has seen any algebraic geometry. Except for a few isolated sections, which can be omitted if desired, we do not assume the reader knows Galois theory. We implicitly use Galois theory for finite fields, but in this case everything can be done explicitly in terms of the Frobenius map so the general theory is not needed. The relevant facts are explained in an appendix.

The book provides an introduction to both the cryptographic side and the number theoretic side of elliptic curves. For this reason, we treat elliptic curves over finite fields early in the book, namely in Chapter 4. This immediately leads into the discrete logarithm problem and cryptography in Chapters 5, 6, and 7. The reader only interested in cryptography can subsequently skip to Chapters 10 and 11, where complex multiplication and the Weil and Tate-Lichtenbaum pairings are discussed. But surely anyone who becomes an expert in cryptographic applications will have a little curiosity as to how elliptic curves are used in number theory. Similarly, a non-applications oriented reader could skip Chapters 5, 6, and 7 and jump straight into the number theory in Chapters 8 and beyond. But the cryptographic applications are interesting and provide examples for how the theory can be used.

There are several fine books on elliptic curves already in the literature. This book in no way is intended to replace Silverman's excellent two volumes [90], [92], which are the standard references for the number theoretic aspects of elliptic curves. Instead, the present book covers some of the same material, plus applications to cryptography, from a more elementary viewpoint. It is hoped that readers of this book will subsequently find Silverman's books more accessible and will appreciate their slightly more advanced approach. The books by Knapp [47] and Koblitz [49] should be consulted for an approach to the arithmetic of elliptic curves that is more analytic than either this book or [90]. For the cryptographic aspects of elliptic curves, there is the recent book of Blake et al. [7], which gives more details on several algorithms than the present book, but contains few proofs. It should be consulted by serious students of elliptic curve cryptography. We hope that the present book provides a good introduction to and explanation of the mathematics used in that book. The books by Enge [28], Koblitz [51], [50], and Menezes [64] also treat elliptic curves from a cryptographic viewpoint and can be profitably consulted.

Notation. The symbols $\mathbf{Z}$, $\mathbf{F}_q$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ denote the integers, the finite field with q elements, the rationals, the reals, and the complex numbers, respectively. We have used $\mathbf{Z}_n$ (rather than $\mathbf{Z}/n\mathbf{Z}$) to denote the integers mod n. However, when p is a prime and we are working with $\mathbf{Z}_p$ as a field, rather than as a group or ring, we use $\mathbf{F}_p$ in order to remain consistent with the notation $\mathbf{F}_q$. Note that $\mathbf{Z}_p$ does not denote the p-adic integers. This choice was made for typographic reasons since the integers mod p are used frequently, while a symbol for the p-adic integers is used only in a few examples in Chapter 13 (where we use $\mathcal{O}_p$). The p-adic rationals are denoted by $\mathbf{Q}_p$. If K is a field, then $\overline{K}$ denotes an algebraic closure of K. If R is a ring, then $R^\times$ denotes the invertible elements of R. When K is a field, $K^\times$ is therefore the multiplicative group of nonzero elements of K. Throughout the book, the letters K and E are generally used to denote a field and an elliptic curve (except in Chapter 9, where K is used a few times for an elliptic integral).

Acknowledgments. The author thanks Bob Stern of CRC Press for suggesting that this book be written and for his encouragement, and the editorial staff at CRC Press for their help during the preparation of the book. Ed Eikenberg, Jim Owings, Susan Schmoyer, Brian Conrad, and Sam Wagstaff made many suggestions that greatly improved the manuscript. Of course, there is always room for more improvement. Please send suggestions and corrections to the author (lcw@math.umd.edu). Corrections will be listed on the web site for the book (www.math.umd.edu/~lcw/ellipticcurves.html).

To Susan and Patrick

Contents